UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,003	03/31/2004	Jerry Chow	NRT.0199US (15392ROUS04U)	5213

21906 7590 05/20/2009

TROP, PRUNER & HU, P.C.
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
05/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,003	CHOW, JERRY	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17,19,20,22-28,30,32,34-36,39,41 and 43-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17,19,20,22-28,30,32,34-36,39,41 and 43-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on 2/12/09.

2. Claims 1-17, 19, 20, 22-28, 30, 32, 34-36, 39, 41 and 43-47 are pending.

Response to Amendment

3. The 101 rejections to claims 1-8, 10, 11, 41 and 46 are withdrawn as the amendment overcomes the 101 rejections. A "memory access manager including at least hardware" is clearly not directed to a software module per se. It is noted that Applicant's specification only describes embodiments of a "memory access manager including at least hardware" as "hardware- or firmware based." See pg. 9, lines 6-8.

Response to Arguments

4. Applicant's arguments with respect to the prior art rejections have been considered but are not persuasive.

5. Applicant argues in substance that the Bryant prior art teaches away from the claimed invention because the "user program stores the token in the register for "future use," i.e. for retrieval when using one of the special instructions." (See Remarks, pgs. 12-14) However, Applicant's analysis ignores relevant features of the prior art. As stated by the Applicant, the Bryant prior art discloses storing the token for a user program such that the program can access the token when the program needs to alter

the contents of a protected page; Bryant also discloses storing corresponding tokens as entries affiliated with each protected page. However, Bryant further discloses:

> [i]n operation, the user program issues a special instruction that *retrieves* the previously stored token from its register. The user program then *presents* a virtual address of the datum in the protected page which the instruction intends to alter and the token to an address translation and protection verification process. See col. 5:56-6:6 [emphasis added].

6. This language clearly teaches accessing the token *from* the register to *present* the token to the protection verification process, which inherently requires storing the token to a volatile memory separate from the aforementioned register for the verification process. The storage of the token in this volatile memory is only required until the instruction to access the protected page is completed. It is with respect to this volatile memory the rejection outlined below is based. For this reason, Applicant's arguments are inadequate.

7. Furthermore, Applicant argues that the rejections under Beukema in view of Bishop do not teach the claimed invention because Beukema does not suggest "any desirability to render this protection key inaccessible by overwriting at least a portion of such protection key." Likewise, Applicant argues that the rejections of England in view of Bishop do not teach the claimed invention because England does not suggest "any desirability of incorporating such a feature." These arguments are not persuasive because they ignore the teaching of Bishop in the 103(a) rejections. The rejections below rely on the teachings of Bishop to suggest the desirability of render a protection key inaccessible by overwriting at least a portion of the protection key. As outlined below, Bishop discloses a basic tenet of secure deletion of sensitive information: "When

a process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released." (pg. 901, last sentence-pg. 902, first sentence, emphasis added) Bishop further discloses an example of erasing sensitive information by overwriting the data. Pg. 902, 1st full paragraph.

8. For these reasons, Applicant's arguments are not persuasive and the claims remain rejected under the prior art of record.

9. Note that the Non-final office action mailed on 11/12/08 had a typographically error in paragraph 12. The rejection heading stated that "Claims 16, 17, 19, 20, 22, 25, 36, 39, 43, 44 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. US 6,976,163 (hereinafter Hind) in view of Bryant." However, as elaborated in the rejection that followed in the 11/12/08 office action, the 103(a) rejections were clearly based on Hind, in view of Bryant and Bishop. See Non-final office action, dated 11/12/08, paragraph 13. The rejection heading below for these rejections has been corrected.

Claim Rejections - 35 USC § 103

10. Claims 1, 9, 10, 22-28, 30, 32, 34, 35, 41 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bryant et al. US 5,628,023 (hereinafter Bryant) in view of Bishop Computer Security, Chapter 29.5 "Common Security-Related Programming Problems" (hereinafter Bishop).

11. As per claims 1, 9, 10, 41 and 46, Bryant discloses a memory protection system comprising:

a. a key store to store identifiers of protected memory locations and respective corresponding memory protection keys; and a memory access manager including at least hardware configured to receive a memory command for altering contents of any of the protected memory locations, determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered wherein the memory protection key in the memory command is written to a volatile memory, if the memory command includes the memory protection key corresponding to each protected memory location to be altered, permit the memory command to proceed, and then render the memory protection key in the memory command inaccessible (col. 5:55-6:20, the token is accessed *from* the register to *present* the token to the protection verification process; fig. 3, reference nos. 485-530 and 535-560; figs. 7 and 9; by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26);

b. implemented in an electronic device having a memory, the memory comprising the protected memory locations and unprotected memory locations (program requests region of memory to be protected);

c. wherein the memory access manager is further configured to receive memory commands for altering contents of the unprotected memory locations

without checking for any memory protection key (only protected memory is verified [see fig. 3]);

d. wherein the memory access manager is configured to further receive a memory read command to read content of a particular protected memory location, the memory access manager to allow the memory read command to proceed to read the content of the particular protected memory location without checking for any memory protection key. (col. 21:3-22)

Although Bryant does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile storage such that the memory protection key written to the volatile memory is inaccessible after completion of the memory command, the step of erasing sensitive information to prevent unauthorized disclosure of protected information is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Bishop discloses a basic tenet of secure deletion of sensitive information: "When a process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released." (pg. 901, last sentence-pg. 902, first sentence, emphasis added) Bishop further discloses an example of erasing sensitive information by overwriting the data. Pg. 902, 1st full paragraph. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory

protection key written to the volatile storage such that the memory protection key written to the volatile memory is inaccessible after completion of the memory command. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 1, 9, 10, 41 and 46.

12. As per claims 22-27, 30, 32, 34 and 35, Bryant discloses a method of protecting memory in an electronic device, comprising:

e. receiving a memory command to access a protected memory location; determining whether the received memory command is a memory read command to read the protected memory location, or a memory write command to alter the protected memory location (col. 21:3-21; fig. 3); in response to determining that the received memory command is the memory write command:

i. identifying a memory protection key corresponding to the protected memory location; determining whether the memory command includes the memory protection key corresponding to the protected memory location, wherein at least the memory protection key in the memory write command has been written to volatile memory; permitting completion of the memory write command if the memory command includes the memory protection key corresponding to the protected memory location (col. 5:55-6:20, the token is accessed *from* the register to *present* the token to the protection verification process; fig. 3, reference nos. 540, 560); and rendering the memory protection key in the memory command that has been written to

the volatile memory inaccessible (by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26); and

f. in response to determining that the received memory command is the memory read command, processing the memory read command to read the protected memory location without checking for any memory protection key; (21:15-18)

g. wherein permitting comprises performing the memory write command (fig. 3, reference no. 570);

h. wherein receiving comprises receiving the memory command from an originating electronic device component, and wherein permitting comprises allowing the originating electronic device component to perform the memory write command; (fig. 1, reference nos. 100, 105, 110)

i. receiving data to be written to the protected memory location; and generating the memory write command responsive to receiving the data (fig. 3, reference no. 540);

j. wherein the received data comprises a received key, and wherein generating comprises extracting the received key from the received data and inserting the received key into the memory write command (fig. 3, reference nos. 540 and 550).

k. Wherein determining comprises comparing the memory protection key corresponding to the protected memory location with the received key in the memory write command (fig. 3, reference nos. 555 and 560).

l. wherein identifying comprises identifying a protected memory location in the memory write command and accessing a mapping table that maps protected memory locations to respective corresponding memory protection keys (fig. 1, reference nos. 140, 145, 155, 175 and 185);

m. further comprising: receiving memory commands to alter unprotected memory locations; and permitting completion of the memory commands to alter unprotected memory locations without checking for any memory protection keys (unprotected memory does not require verification);

n. wherein the identifying step comprises accessing the memory protection key corresponding to the protected memory location in a key store, the method further comprising:

ii. receiving a command to establish a new protected memory location in the memory and a memory protection key corresponding to the new protected memory location; establishing the new protected memory location in the memory; and storing the memory protection key in the key store. (fig. 3, reference nos. 485-530; figs. 7 and 9)

o. Bryant further discloses a computer-readable medium storing instructions for performing the method of claim 22. (fig. 1)

Although Bryant does not disclose rendering the memory protection key in the memory command that has been written to the volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory

inaccessible after completion of the memory write command, the step of erasing sensitive information to prevent unauthorized disclosure protected information is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Bishop discloses a basic tenet of secure deletion of sensitive information: "When a process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released." (pg. 901, last sentence-pg. 902, first sentence, emphasis added) Bishop further discloses an example of erasing sensitive information by overwriting the data. Pg. 902, 1st full paragraph. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command that has been written to the volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory inaccessible after completion of the memory write command. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 22-27, 30, 32, 34 and 35.

13. As per claim 28, the rejection of claim 26 under 35 USC 103(a) as being unpatentable over Bryant in view of Bishop is incorporated herein. Neither Bryant nor Bishop expressly disclose wherein determining comprises retrieving a modified version

of the memory protection key corresponding to the protected memory location, modifying the received key in the memory write command to generate a modified received key, and comparing the modified received key to the modified version of the memory protection key corresponding to the protected memory location. However, it is notoriously well known in the art to use and store a hash value of an identifier as opposed to the original identifier. A hash value uniquely maps an original value to a modified value, such that the modified value is typically much smaller than the original value. Hence, the modified value retains the unique property of the original value but requires less memory and bandwidth requirements to store and communicate the value. Official Notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the determining step comprises retrieving a modified version of the memory protection key corresponding to the protected memory location, modifying the received key in the memory write command to generate a modified received key, and comparing the modified received key to the modified version of the memory protection key corresponding to the protected memory location. One would be motivated to do so to preserve memory and processing resources as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 28.

14. Claims 1, 2, 4, 7-9, 11-15 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beukema et al. US Patent Application Publication No. 20020124148 (hereinafter Beukema) in view of Bishop.

15. As per claims 1, 2, 4, 7-9, 11-15 and 46, Beukema discloses a memory protection system comprising:

p. a key store to store identifiers of protected memory locations and respective corresponding memory protection keys; and a memory access manager including at least hardware configured to receive a memory command for altering contents of any of the protected memory locations, determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, wherein the memory protection key in the memory command is written to a volatile memory, if the memory command includes the memory protection key corresponding to each protected memory location to be altered, permit the memory command to proceed, and then render the memory protection key in the memory command inaccessible (paragraph 54; by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26);

q. wherein the identifiers comprise addresses in a protected memory; wherein the identifiers identify data entries in a protected memory; (paragraph 54; pointer to an associated memory region/address)

r. wherein the key store stores a mapping table that maps each identifier to a corresponding memory protection key; (paragraph 54; "Protection/Translation Table");

s. wherein at least one of the identifiers is mapped to multiple corresponding memory protection keys (paragraph 54; L_key and R_key);

t. the system implemented in an electronic device having a memory, the memory comprising the protected memory locations and unprotected memory locations (paragraph 55, and fig. 6);

u. wherein the memory access manager is further configured to perform the memory command that includes the memory protection key corresponding to each protected memory location to be altered (paragraphs 54 and 59);

v. the system implemented in an electronic device, wherein the memory command is received by the memory access manager from an originating electronic device component, and wherein the originating electronic device component proceeds with the memory command permitted by the memory access manager; wherein the originating electronic device component is a memory update module; wherein the originating electronic device component sends memory commands to the memory access manager responsive to data received at the electronic device; wherein the originating electronic device component is further configured to extract a received memory protection key from the received data and to provide the received memory protection key to the memory access manager. (fig. 2; paragraphs 54-56; external user supplies protection key for rights access (read, write) to protected memory)

Although Beukema does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile storage such that the memory protection key written to the volatile memory is inaccessible after completion of the memory write command,

the step of erasing sensitive information to prevent unauthorized disclosure protected information is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Bishop discloses a basic tenet of secure deletion of sensitive information: "When a process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released." (pg. 901, last sentence-pg. 902, first sentence, emphasis added) Bishop further discloses an example of erasing sensitive information by overwriting the data. Pg. 902, 1st full paragraph. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile memory is inaccessible after completion of the memory write command. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 1, 2, 4, 7-9, 11-15 and 46.

16. Claims 16, 17, 19, 20, 22, 25, 36, 39, 43-45 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. US 6,976,163 (hereinafter Hind) in view of Bryant and Bishop.

17. As per claims 16, 17, 19, 20 and 43, Hind discloses an electronic device comprising a memory; a wireless receiver configured to receive data relating to a

remote software update to be written to the memory, and means to securely update the software files via update rules. (col. 2:38-59; 19:40-46) However, Hind does not disclose ensuring that the update has the proper permission to execute the update in a particular memory region. Bryant discloses an electronic device comprising:

w. a memory; a receiver configured to receive data to be written to the memory; and a memory protection system associating protected memory locations in the memory with respective corresponding keys, and configured to allow the received data to be written to any of the protected memory locations only if the received data includes a key corresponding to the protected memory location to which the received data is to be written and to render the corresponding key in the received data inaccessible after allowing the received data to be written to the protected memory location (fig. 1, fig. 3);

x. volatile storage having unprotected memory locations, the memory protection system configured to download the received data including the key to the unprotected memory locations of the volatile storage prior to writing the received data to the protected memory locations; wherein the volatile storage is part of the memory (fig. 1, reference nos. 125, 130 and 140);

y. wherein each key is rendered inaccessible by erasing the received data from the unprotected memory locations where the memory access manager allows the received data to be written to the protected memory locations (by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26);

z. wherein the memory protection system comprises: a key store storing a mapping table that associates the protected memory locations with the respective corresponding keys; and a memory access manager configured to process a memory command for writing the received data to any of the protected memory locations, determine whether the received data includes the key corresponding to any of the protected memory locations to which the received data is to be written, if the received data includes the key corresponding to a protected memory location to which the received data is to be written, to permit the memory command to proceed, and then render the corresponding key in the received data inaccessible (19:41-20:6);

aa. wherein the key store resides at a secure location in the memory outside of the main memory (fig. 1, reference no. 105);

bb. wherein the memory protection system is configured to further receive a memory read command to access a particular one of the protected memory locations, perform reading of the particular protected memory location in response to the memory read command, without checking for any memory protection key. (21:3-22)

It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Hind with the teaching of Bryant. One would be motivated to do so to ensure that the update has the proper permission to execute the update in a particular memory region as disclosed by Bryant. (5:22-30)

Furthermore, although Bryant does not disclose the memory protection system to render the key inaccessible by overwriting at least a portion of the key, the step of erasing sensitive information to prevent unauthorized disclosure protected information is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Bishop discloses a basic tenet of secure deletion of sensitive information: "When a process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released." (pg. 901, last sentence-pg. 902, first sentence, emphasis added) Bishop further discloses an example of erasing sensitive information by overwriting the data. Pg. 902, 1st full paragraph. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the memory protection system to render the key inaccessible by overwriting at least a portion of the key. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 16, 17, 19, 20 and 43.

18. As per claims 22, 25 and 44, Hind discloses a method to remotely update software via update rules contained in the update; receiving the update comprises receiving, by a wireless receiver. (col. 2:38-59; 19:40-46) However, Hind does not disclose ensuring that the update has the proper permission to execute the update in a particular memory region. Bryant discloses a method of protecting memory in an electronic device, comprising:

cc. receiving a memory command to access a protected memory location; determining whether the received memory command is a memory read command to read the protected memory location, or a memory write command to alter the protected memory location (col. 21:3-21; fig. 3); in response to determining that the received memory command is the memory write command:

iii. identifying a memory protection key corresponding to the protected memory location; determining whether the memory command includes the memory protection key corresponding to the protected memory location, wherein at least the memory protection key in the memory write command has been written to volatile memory; permitting completion of the memory write command if the memory write command includes the memory protection key corresponding to the protected memory location (col. 5:55-6:20, the token is accessed *from* the register to *present* the token to the protection verification process; fig. 3, reference nos. 540, 560); and rendering the memory protection key in the memory command that has been written to the volatile memory inaccessible (by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26); and

dd. in response to determining that the received memory command is the memory read command, processing the memory read command to read the protected memory location without checking for any memory protection key; (21:15-18)

ee. receiving data to be written to the protected memory location; and generating the memory write command responsive to receiving the data (fig. 1, reference no. 540);

It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Hind with the teaching of Bryant. One would be motivated to do so to ensure that the update has the proper permission to execute the update in a particular memory region as disclosed by Bryant. (5:22-30)

Finally, although Bryant does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory inaccessible after completion of the memory write command, the step of erasing sensitive information to prevent unauthorized disclosure protected information is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Bishop discloses a basic tenet of secure deletion of sensitive information: "When a process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released." (pg. 901, last sentence-pg. 902, first sentence, emphasis added) Bishop further discloses an example of erasing sensitive information by overwriting the data. Pg. 902, 1st full paragraph. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command

inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory inaccessible after completion of the memory write command. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill.

The aforementioned cover the limitations of claims 22, 25 and 44.

19. As per claims 36, 45 and 47, Hind discloses a method to remotely update software via update rules contained in the update; wherein the update is received by a wireless receiver. (col. 2:38-59; 19:40-46) However, Hind does not disclose ensuring that the update has the proper permission to execute the update in a particular memory region. Bryant discloses a method of protecting electronic memory, comprising:

ff. configuring a memory store of an electronic device into at least one protected memory location and a key store operable to store an identifier of each protected memory location and a respective corresponding memory protection key; and configuring a processor of the electronic device to provide a memory access manager operable to receive memory commands for altering contents of any of the at least one protected memory location, and for at least one memory command, to :determine whether the at least one memory command includes a memory protection key corresponding to at least one protected memory location to be modified, said memory command including the memory protection key corresponding to at least one said protected memory location to be modified,

permit the at least one memory command and then render each corresponding memory protection key in the at least one memory command inaccessible; wherein the memory protection key in the at least one memory command is written to volatile memory, and wherein the memory protection key in the at least one memory command is rendered inaccessible (col. 5:55-6:20, the token is accessed *from* the register to *present* the token to the protection verification process; fig. 3, reference nos. 540-570; by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26)

gg. wherein configuring the processor further comprises configuring the processor to receive a memory read command to read a particular one of the protected memory locations, and to permit the memory read command to read the particular protected memory location without checking for any memory protection key. (21:3-22)

It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Hind with the teaching of Bryant. One would be motivated to do so to ensure that the update has the proper permission to execute the update in a particular memory region as disclosed by Bryant. (5:22-30)

Finally, although Bryant does not disclose rendering the memory protection key in the at least one memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile memory such that the memory protection key written to the volatile memory is rendered inaccessible after completion of the at least one memory command, the step of erasing sensitive information to

prevent unauthorized disclosure protected information is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Bishop discloses a basic tenet of secure deletion of sensitive information: "When a process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released." (pg. 901, last sentence-pg. 902, first sentence, emphasis added) Bishop further discloses an example of erasing sensitive information by overwriting the data. Pg. 902, 1st full paragraph. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the at least one memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile memory such that the memory protection key written to the volatile memory is rendered inaccessible after completion of the at least one memory command. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 36, 45 and 47.

20. As per claim 39, Bryant further suggests a computer-readable medium storing instructions for performing the method of claim 36. (fig. 1)

21. Claims 1 and 3-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over England et al. USPN 7,194,092 (hereinafter England) in view of Bishop.

22. As per claims 1 and 3-6, England discloses a memory protection system comprising:

hh. a key store to store identifiers of protected memory locations and respective corresponding memory protection keys; and a memory access manager including at least hardware configured to receive a memory command for altering contents of any of the protected memory locations, determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, wherein the memory protection key in the memory command is written to a volatile memory, if the memory command includes the memory protection key corresponding to each protected memory location to be altered, permit the memory command to proceed, and then render the memory protection key in the memory command inaccessible (col. 10:41-51, when an application wants to access protected stored content, the application passes its rights manager certificate and storage key to the DRMOS, storage of the storage key in volatile memory is inherent in this step; by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26);

ii. wherein the identifiers comprise names of protected files in a memory; wherein the identifiers identify data entries in a protected memory; (10:31-35; 16:33-37)

jj. wherein each of the memory protection keys comprises a modified version of a data sequence; wherein the modified version comprises a hash of the data sequence. (10:41-51; 17:1-30; 17:57-18:14)

23. Although England does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile storage such that the memory protection key written to the volatile memory is inaccessible after completion of the memory command, the step of erasing sensitive information to prevent unauthorized disclosure protected information is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Bishop discloses a basic tenet of secure deletion of sensitive information: "When a process finishes using a sensitive object (one that contains confidential information or one that should not be altered), the object should be erased, then deallocated or deleted. Any resources not needed should also be released." (pg. 901, last sentence-pg. 902, first sentence, emphasis added) Bishop further discloses an example of erasing sensitive information by overwriting the data. Pg. 902, 1st full paragraph. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile memory is inaccessible after completion of the memory command. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 1 and 3-6.

Conclusion

24. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUNG KIM whose telephone number is (571)272-3804. The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432